



Outlook

Audit Committee Meeting Public comment

From January Walker <january@infoton.ai>

Date Sun 9/20/2026 8:05 PM

To publicinput@tooeleco.gov <publicinput@tooeleco.gov>

1 attachment (826 KB)

CyberAtomsics- Computational Thermodynamic Weapons of Mass Destruction Posing as Digital Assets.pdf;

*Traditional cybersecurity audits focus on firewall logs and software patches. As learned at a major financial firm however, the deepest, most complex cyber risks overlap directly with the state's physical energy architectures and our financial line items. Malicious software and un-vetted high-capacity computational platforms (like speculative data centers) act as autonomous engines that consume massive energy, decay infrastructure, and **waste entropy at scale**.*

*Because these systems cannot hide their physical footprint, **examining the intersection of utility costs, infrastructure wear, and asset depreciation is one of our most reliable ways to detect systemic cyber anomalies**. We cannot treat energy proposals and technology proposals as separate silos; a surge in physical utility stress translates directly to a material financial risk to taxpayers.*

As such, my questions for the Auditing firm are as follows.

*1, Within your testing of our **Internal Controls Over Financial Reporting (ICFR)**, can we establish a baseline protocol where unexpected variance or spikes in our power grid utility expenditures are flagged as potential cybersecurity indicators even at the tiniest levels? Since cyber-attacks and high-entropy processing put excessive, un-budgeted wear on regional energy grids, how will the audit team reconcile physical utility data with our digital risk posture?*

2, As new data center proposals are evaluated by the county, their unprecedented utility draw risks triggering localized grid saturation and thermal stress. From a capital asset perspective, how will the audit evaluate the risk of accelerated degradation on local government-owned infrastructure (such as regional power hubs or cooling water resources) before these proposals are financially approved?

*3, If malicious actors or un-vetted background processes are running unauthorized, high-entropy workloads inside our architecture, they leave a financial paper trail in the form of compressed asset life and inflated operational overhead. Will your audit protocols look at **hardware depreciation anomalies** as a forensic tool to check for unauthorized or compromised system operations?*

4, You ask for a baseline of \$57,413.02, with a 4% annual compound escalation rate. \$287,065.09 divided by 5 is \$57,413.02, I propose each percentage be tied to quantum accounting which tracks the financial connection to money, entropy, and the Great Salt Lake water levels as catching those exploiting county infrastructure and costing taxpayers' money is at the heart of the problem with little awareness and visibility today.

With the Data Center proposals, that level of accountability will be needed. A printout of the above report—even in color may be of value to the firm being evaluated as the spread of miners has already entered into Tooele County energy infrastructure and is putting undue, and unaccounted for tax burden today. An energy and data scaling line item which left unaudited allows for liabilities to be shifted onto unsuspecting taxpayers instead of technologists and banks where they belong. The similarity is much like Amazon switching to electric to bypass the gas tax while continuing to use roads.

January N. Walker

Executive, PISO

ORCID: [0009-0000-6843-2051](https://orcid.org/0009-0000-6843-2051)

<https://infoton.ai/>